September 2018

PEXA, email, electronic funds transfers and cyber-crime

On 25 June 2018 LPLC published a security warning for PEXA users arising from some recent instances of fraudulent activity impacting PEXA transactions.

One of these ('the MasterChef case') involved a fraudster entering the PEXA workspace and changing payment account details to divert $250,000 of the proceeds of sale into another bank account controlled by the fraudster.

The fraudster initially compromised the conveyancer's email account, intercepted a password reset email and gained access to the conveyancer's PEXA account. They then created a new user profile, obtained new user credentials, accessed a workspace, and changed payment data previously entered by the conveyancer.

The risk of EFT-fraud for lawyers is human error, not IT

Lawyers are not responsible for any technical shortcomings in PEXA's platform or security weaknesses within the broader banking system, but they are responsible for the data they enter into the workspace and for checking its correctness before applying the digital signature and authorising a settlement to proceed.

1. It starts with email security – recognise that you will be subject to phishing attacks and social engineering techniques. Typically, you may be asked to click on unsafe hyperlinks or open attachments from legitimate looking sources which introduce malware to your computer or trick you into visiting a fake login page of a trusted website and enter username and password details.
2. Once an email account is compromised, cyber-criminals have numerous techniques and tools at their disposal to obtain password information and it is just a matter of time before they discover the password(s) you use to access your online accounts.
3. Password access to online accounts is akin to having the keys to your house. But in PEXA there is a further step before a cyber-criminal can steal money or complete a fraudulent property transaction – that step involves the application of a digital signature to execute instruments and to certify the correctness of all dealings. A cyber-criminal with password access to the workspace alone cannot transact on the account – they can only enter and

save data in the workspace. Only a user holding a digital certificate and signing rights can sign registry instruments and financial settlement schedules and, critically, authorise settlements to proceed. In the MasterChef case the conveyancer authorised the payment via PEXA's platform without noticing that the payment details had been altered.

4. Digital certificates are such important security devices that they should only be given to very trusted people within your firm. You carefully select the people you authorise as signatories to your trust account, and at least the same care is needed when granting digital certificate access rights. Holders of a digital certificate must store it safely and not share access credentials with others.

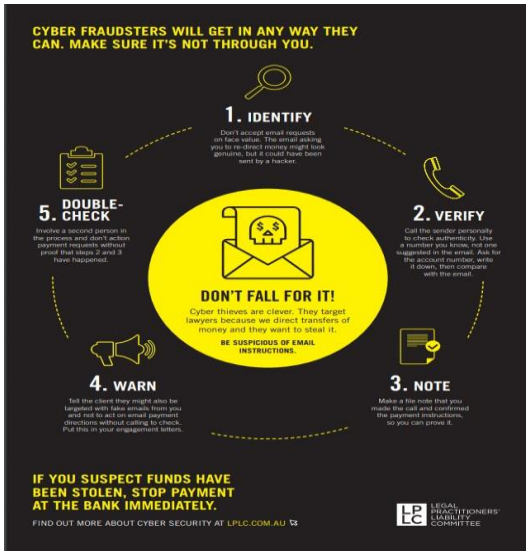
The major liability risks for legal practitioners arising from the use of PEXA are thus not IT risks. Rather, they are risks arising from **human error** in entering and checking workspace details, or lapses in security resulting in misuse of a digital certificate.

Keeping the digital certificate secure, not 'lending' it out, and being diligent to ensure the accuracy of all disbursement entries in the financial settlement schedule are critical to successfully navigating liability risks with PEXA transactions.

Verify all email instructions for the transfer of funds

The MasterChef case was a sophisticated fraud, though ultimately simple in its execution. It is a powerful reminder of the need to exercise extreme care with any electronic funds transfers, including PEXA transactions.

Remember LPLC's 5-step process for managing the risk of being caught by fraudulent email instructions



If you become aware funds have been stolen, stop payment at the bank immediately.

LPLC's 5-step process

1. Identify – Don't accept email requests on face value. The email asking you to re-direct money might look genuine, but it could have been sent by a hacker.

2. Verify – Call the sender personally to check authenticity. Use a number you know, not one suggested in the email. Ask for the account number, write it down, then compare with the email.

3. Note – Make a file note that you made the call and confirmed the payment instructions, so you can prove it.

4. Warn – Tell the client they might also be targeted with fake emails from you and not to act on email payment directions without calling to check. Put this in your engagement letters.

5. Double-check – Involve a second person in the process and don't action payment requests without proof that steps 2 and 3 have happened.

Always double-check bank account details before sign-off

Electronic payment platforms relying solely on the manual entry of correct bank account numbers are inherently vulnerable to human error.

You must remain alert to this risk and ensure bank account numbers entered in a PEXA workspace accord **precisely** with the client's instructions. This requires:

- clear evidence of the client's instructions, with verification by telephone if the instructions are via email
- careful data entry in the workspace, and
- a work-system for double-checking the data entry.

A good way to double-check is to involve a second person in the process. Have a work system where one person inputs the account details and a second person checks them and signs the settlement schedule.

PEXA residential seller's guarantee

PEXA recently announced a Residential Seller Guarantee (the guarantee) to allay consumer concerns about the security of its electronic platform. PEXA's explanation about the guarantee is available on its website.

LPLC has received several enquiries about the operation of the guarantee.

What the PEXA residential seller guarantee covers

The guarantee:

- is confined to residential property sales by sellers who are not registered or required to be registered for GST
- will operate only where a fraudster gains access to the PEXA platform and changes **correctly entered** bank account details, resulting in money being sent to the fraudster's account.

The amount payable under the guarantee is limited to specified losses and subject to a cap of $2m. It does not cover any consequential losses and it excludes mortgage payments, rates, taxes, property outgoings, conveyancer fees and any loss involving dishonest or fraudulent conduct by the seller's practitioner.

Three-day time limit for seller to apply for guarantee

You must note the **three-day time limit** for making a claim for payment under the guarantee. This can only be extended by PEXA in its absolute discretion.

The claim form for the guarantee is available on the PEXA website and must be completed by both the seller (Part A), the seller's practitioner/subscriber (Part B) and submitted to PEXA within three business days of the fraudulent transaction.

Completion of Part B by you will not jeopardise your entitlement to indemnity under LPLC's insurance policy.

PEXA may exercise its rights of subrogation to claim back any money it pays to the seller under the guarantee if PEXA considers you or your authorised signer was negligent in approving a settlement containing incorrect bank payment details.

You will need to consider any conflict of interest in accordance with the rules of professional conduct.

What to do if EFT fraud is discovered in a PEXA transaction

1	Immediately telephone both the disbursing and receiving banks (and follow up with written confirmation) to report the theft and request the account be frozen.	
2	Inform PEXA immediately on **1300 084 515**. It will also contact the banks and may be able to get action taken more quickly to stop the withdrawal of stolen funds.	
3	Inform the seller about the PEXA residential seller guarantee and provide them with copy of the PEXA claim form for completion. Advise the client of the three-day time limit for making a claim under the guarantee.	
4	Consider whether you have a conflict in continuing to act for the seller (for example, if there is a potential claim against you in relation to the entry or checking of bank account details in the financial settlement schedule) and if so, refer the client to another solicitor for independent legal advice.	
5	If the seller wishes to make a claim under the PEXA guarantee complete Part B (practitioner's part) of the claim form, making sure all answers are factually correct.	
6	Notify LPLC of the potential for a claim as soon as possible and provide us with a copy of the completed PEXA claim form.	
7	Report the cybercrime to police and to ACORN.	

For more information on how to protect your firm from cyber-attacks see the material on the cyber page on our website and in particular our Cyber security checklist.